Egregore Nomad-Cryptography (ENC): A Whitepaper for Experimental Counter-economics

Razi Nakamoto, Hamdan Muhammad, Dadang Rukmana,
Lain Wilson, Sanda Selamba, Pierre Renura,
Trazianziejkamnanazjire Muhammad Syuhada
studiolarang@riseup.net

Diterjemah ke dalam bahasa Indonesia
oleh
John A. C.

Abstrak. Dokumen ini menguraikan kerangka kerja konseptual dan teknis untuk Egregore Nomad-Cryptography (ENC), sebuah sistem sosio-ekonomi otonom yang dirancang untuk operasi skala lokal oleh para konspirator afinitas. Dengan mensintesis prinsip-prinsip Mutualisme Proudhonian, taktik penghilangan dari Zona Otonom Temporer (TAZ), dan etos operasional Pascakonspirasi, model ini menolak struktur hierarkis dan ketergantungan pada negara-kapital. Arsitektur ekonomi didasarkan pada alokasi surplus yang dihitung melalui model Valuasi Kontribusi Multi-Atribut, memastikan distribusi yang adil berdasarkan input kuantitatif dan kualitatif. Tata kelola dijalankan melalui mekanisme konsensus berbasis reputasi dinamis yang menolak tirani mayoritas dari sistem voting (pemilihan). Infrastruktur teknis dibangun di atas tumpukan terdesentralisasi, memanfaatkan *blockchain* untuk perbendaharaan (kas) yang transparan dan tahan sensor, dengan analisis komparatif aset kripto privat (misalnya, Monero) dan *stablecoin* terdesentralisasi (misalnya, DAI). Sistem ini diperkuat dengan kriptografi canggih seperti zk-SNARKs untuk verifikasi privat dan mengintegrasikan Agen Ekonomi Otonom (AEA) untuk otomatisasi tugas dan efisiensi operasional. Kerangka kerja ini diakhiri dengan panduan Keamanan Operasional (OPSEC) yang disesuaikan untuk aktivitas klandestin, menyajikan sebuah cetak biru yang holistik dan dapat ditindaklanjuti untuk eksperimen dalam otonomi radikal.

1 Pendahuluan

1.1 Konteks Eksperimental

Proyek yang diuraikan dalam dokumen ini, yang diinisiasi oleh para eksperimentalis yang berafiliasi dengan Studio Larang, secara fundamental bukanlah sebuah manifesto politik atau cetak biru untuk revolusi total.

Sebaliknya, ia harus dipahami sebagai sebuah *eksperimen dalam kesenangan dan penolakan*. Pendekatan ini secara sadar menjauhkan diri dari retorika grandiosa yang sering kali menyertai proyek-proyek utopis, yang menurut Djoedibarie sering kali "berakhir dengan membangun penjara baru dengan jeruji yang lebih indah". Alih-alih berfokus pada pembangunan masa depan yang abstrak, eksperimen ini berakar pada intensifikasi kehidupan di sini dan sekarang. Ia mengambil inspirasi dari proklamasi Nietzsche, "Saya datang sebagai Dionysus yang menang, yang akan mengubah dunia menjadi hari libur". Dalam semangat ini, tindakan menciptakan otonomi ekonomi bukanlah sebuah tugas yang suram, melainkan sebuah tindakan afirmatif yang penuh kegembiraan—sebuah upaya untuk merebut kembali bukan hanya nilai kerja, tetapi juga kesenangan dalam hidup dan berkreasi di luar batasan-batasan yang dipaksakan.

Para partisipan dalam eksperimen ini tidak mengidentifikasi diri mereka sebagai aktivis atau revolusioner dalam pengertian tradisional; mereka adalah para *konspirator* dan *eksperimentalis* yang sedang bersenang-senang. Kesenangan ini ditemukan dalam proses penemuan, dalam pembajakan ruang dan alat, dan dalam penciptaan hubungan sosial baru yang tidak dimediasi oleh kekuasaan atau keuntungan. Dengan demikian, keberhasilan proyek ini tidak diukur dari kemampuannya untuk menggulingkan sistem yang ada, tetapi dari kemampuannya untuk menciptakan "enklave bebas" yang bersifat sementara di mana individu dapat mengalami otonomi absolut dan interaksi manusia yang bebas dan tidak termediasi, bahkan jika hanya untuk sesaat. Ini adalah praktik *anarki ontologis*: realisasi kebebasan dalam tindakan itu sendiri, bukan penantian tanpa akhir untuk sebuah revolusi yang mungkin tidak akan pernah datang.

1.2 Penolakan terhadap Dikotomi Bos-Pekerja

Penolakan terhadap terminologi "bos" dan "pekerja" adalah inti dari etos eksperimen ini. Ini bukan sekadar preferensi semantik, melainkan penolakan filosofis yang mendalam terhadap hubungan kekuasaan yang melekat dalam dikotomi tersebut. Dalam kerangka kapitalisme, hubungan bos-pekerja secara inheren bersifat hierarkis dan eksploitatif. Ia mereduksi individu menjadi fungsi ekonomi—baik sebagai pengarah (kapital) maupun sebagai yang diarahkan (tenaga kerja). Hubungan ini, menurut Proudhon, adalah bentuk perampokan di mana nilai yang diciptakan oleh pekerja diambil oleh pemilik properti atau kapital.

Dari perspektif anarkis-individualis dan egois, yang sangat relevan dengan kerangka kerja ini, setiap struktur yang menempatkan kehendak satu individu di atas yang lain adalah bentuk penindasan. Istilah "pekerja" menyiratkan subordinasi, sementara "bos" menyiratkan dominasi. Keduanya meniadakan otonomi dan kebebasan individu, yang merupakan prinsip tertinggi. Eksperimen Studio Larang berusaha untuk melampaui hubungan ini dengan menciptakan asosiasi individu-individu yang setara, yang bekerja sama berdasarkan kesepakatan sukarela dan saling menguntungkan, bukan karena paksaan ekonomi. Di sini, tidak ada yang memerintah dan tidak ada yang diperintah; yang ada hanyalah para konspirator yang berkolaborasi dalam proyek-proyek yang mereka pilih sendiri. Ini adalah manifestasi praktis dari prinsip “pengelolaan dan koordinasi tanpa

hubungan memerintah dan diperintah". Dengan menolak label-label ini, para konspirator menolak seluruh struktur kekuasaan yang mereka wakili, membuka jalan bagi mode produksi yang benar-benar otonom, non-hierarkis, dan radikal.

1.3 Pengenalan Egregore Nomad-Cryptography (ENC)

Untuk memberikan nama pada sistem yang secara sadar menolak label-label seperti "organisasi" atau "kolektif" , kami mengusulkan istilah *Egregore Nomad-Cryptography atau* ENC.

Egregore adalah sebuah konsep yang berasal dari tradisi esoterisme Barat, yang didefinisikan sebagai entitas atau thoughtform non-fisik yang muncul dari pikiran dan emosi kolektif dari sekelompok individu yang berbeda. Ini adalah metafora yang tepat untuk menggambarkan bagaimana Studio Larang beroperasi. Ia bukanlah sebuah organisasi formal dengan struktur, keanggotaan, atau hierarki yang kaku. Sebaliknya, ia adalah sebuah kesadaran bersama yang cair, sebuah medan gaya psikis yang dihidupkan oleh afinitas dan tindakan bersama para konspiratornya. Egregore ini ada selama para konspirator bertindak bersama, dan menghilang ketika mereka tidak melakukannya. Ia tidak memiliki pusat kendali; ia adalah fenomena emergent yang lahir dari interaksi terdesentralisasi. Penggunaan istilah ini secara strategis menggeser kerangka dari struktur fisik ke kesadaran bersama, selaras dengan penekanan Hakim Bey pada "anarki ontologis" dan penolakan Pascakonspirasi terhadap semua bentuk organisasi formal.

Istilah *Nomad-Cryptography* atau Kriptografi-Nomaden menyatukan dua pilar utama dari kerangka kerja ini. "Kripto" menunjuk pada infrastruktur teknis yang mendasarinya: penggunaan kriptografi, blockchain, dan teknologi keuangan terdesentralisasi (DeFi) untuk menciptakan sistem ekonomi yang aman, transparan, dan tahan terhadap kontrol eksternal. "Nomaden" merujuk pada filosofi operasionalnya, yang diambil langsung dari konsep "nomadisme psikis" Hakim Bey. Egregore ini tidak terikat pada satu tempat, taktik, atau ideologi. Ia terus bergerak, beradaptasi, dan berevolusi. Ia mendirikan zona otonom temporer (TAZ), baik di dunia fisik maupun di dunia digital (*smart contract* di *blockchain*), dan kemudian menghilang sebelum dapat dipetakan, dikendalikan, atau dihancurkan oleh kekuasaan negara-kapital.

Dengan demikian, *Egregore Nomad-Cryptography* adalah nama untuk sebuah praktik—sebuah metode untuk menjadi dan bertindak bersama secara otonom—bukan nama untuk sebuah kelompok atau institusi. Ini adalah cetak biru untuk sebuah entitas yang hidup di celah-celah, yang kekuatannya terletak pada kemampuannya untuk menghilang.

2 Landasan Konseptual

Kerangka kerja *Egregore Nomad-Cryptography* tidak muncul dari ruang hampa. Ia berdiri di atas bahu dua pilar konseptual yang radikal: taktik penghilangan yang diartikulasikan oleh Hakim Bey dalam *T.A.Z.: The Temporary Autonomous Zone*, dan etos operasional klandestin yang diuraikan oleh Itjang Djoedibarie dalam

Pascakonspirasi. Sintesis dari kedua teks ini membentuk DNA filosofis dari eksperimen ini.

2.1 Taktik Penghilangan Hakim Bey

Hakim Bey (nama pena dari Peter Lamborn Wilson) memberikan alternatif yang kuat terhadap model revolusi frontal yang dianggapnya sudah usang dan kontra-produktif. Alih-alih konfrontasi langsung dengan Negara—sebuah konfrontasi yang hampir pasti akan kalah atau, jika menang, hanya akan melahirkan Negara yang lebih represif—Bey mengusulkan serangkaian taktik yang berpusat pada penghindaran, ketidakterlihatan, dan penciptaan ruang-ruang kebebasan yang bersifat sementara.

2.1.1 Zona Otonom Temporer (TAZ)

TAZ adalah konsep sentral Bey, yang didefinisikan sebagai praktik untuk menghindari struktur kekuasaan formal melalui kombinasi pembebasan psikologis dan taktik sosio-politik. TAZ bukanlah sebuah utopia permanen yang harus dipertahankan sampai mati. Sebaliknya, ia adalah "pemberontakan yang tidak terlibat langsung dengan Negara; ia membebaskan sebuah area (tanah, waktu, imajinasi) dan kemudian ia larut untuk membentuk dirinya kembali di tempat lain/waktu lain, sebelum Negara dapat menghancurkannya". Bagi Studio Larang, setiap proyek—baik itu mencetak batch kaos, menerbitkan zine, atau meluncurkan produk digital—adalah sebuah TAZ. Ruang dan waktu yang didedikasikan untuk proyek tersebut menjadi zona otonom di mana aturan-aturan dunia luar (kerja upahan, hierarki, kepemilikan intelektual) ditangguhkan. Setelah proyek selesai dan surplus didistribusikan, TAZ tersebut "menghilang", hanya menyisakan artefak dan jejak ingatan. TAZ bukanlah tujuan akhir, melainkan sebuah kesempatan untuk mengalami kualitas hidup yang lebih tinggi yang terkait dengan pemberontakan—sebuah kilasan utopia pasca-revolusi tanpa harus melalui kekerasan revolusi itu sendiri.

2.1.2 Invisibilitas dan Penghilangan (Invisibility and Disappearance)

Kekuatan terbesar TAZ, menurut Bey, adalah invisibilitas-nya. Negara tidak dapat mengontrol apa yang tidak dapat dilihatnya, dan TAZ ada "di luar definisi, di luar pandangan dan penamaan sebagai tindakan perbudakan". Taktik penghilangan ini adalah strategi sadar untuk menghindari kooptasi dan represi. Begitu sebuah TAZ menjadi terlalu terlihat, terlalu terdefinisi, ia menjadi target. Oleh karena itu, *Egregore Nomad-Cryptography* harus secara aktif mempraktikkan seni menghilang. Secara praktis, ini berarti menjaga keamanan operasional (OPSEC) yang ketat (seperti yang dibahas dalam Bab 7), meminimalkan jejak digital dan fisik, dan menghindari publisitas yang tidak perlu. Operasi harus bersifat klandestin, tidak hanya karena ilegalitas beberapa tindakannya (seperti pembajakan), tetapi juga sebagai prinsip strategis fundamental.

2.1.3 Nomadisme Psikis

Untuk dapat terus bergerak dan menghilang, para konspirator harus mengadopsi apa yang disebut Bey sebagai "nomadisme psikis". Ini adalah sebuah pergeseran dari pandangan dunia yang kaku dan ideologis ke sebuah sikap yang cair dan multi-perspektif. Seorang nomaden psikis tidak terikat pada satu dogma; mereka adalah "pengembara yang didorong oleh keinginan atau rasa ingin tahu, dengan loyalitas yang dangkal... dalam mencari keberagaman dan petualangan". Bagi Studio Larang, ini berarti fleksibilitas radikal. Para konspirator harus bersedia menggunakan alat apa pun yang tersedia—dari mesin sablon tua hingga *smart contract* canggih, dari filsafat Prancis hingga manual OPSEC militer—**tanpa menjadi pengikut setia dari salah satunya.** Nomadisme psikis memungkinkan *Egregore* untuk beradaptasi dengan cepat, memanfaatkan peluang yang muncul, dan meninggalkan taktik yang tidak lagi efektif. Ini adalah penolakan terhadap purisme ideologis demi efektivitas praktis dalam mengejar otonomi.

2.1.4 Terorisme Puitis

Bey juga memperkenalkan konsep "Terorisme Puitis" (PT), yaitu tindakan yang bertujuan untuk menciptakan "kejutan estetika" dan mengganggu realitas konsensus, bukan untuk menyebabkan kerusakan fisik. PT adalah seni sebagai kejahatan; kejahatan sebagai seni. Dalam konteks Studio Larang, produk-produk yang dihasilkan—kaos dengan slogan subversif yang dicetak dengan alat bajakan, buku-buku yang isinya menantang norma-norma yang ada—dapat dilihat sebagai artefak Terorisme Puitis. Mereka lebih dari sekadar komoditas untuk dijual. Mereka adalah intervensi dalam lanskap budaya, tindakan ilegal yang menyebarkan ide-ide dan menciptakan momen-momen keretakan dalam matriks kontrol. Tujuan dari PT, tulis Bey, adalah perubahan. "Jika PT tidak mengubah hidup seseorang (selain seniman), itu gagal". Setiap produk *Egregore* harus bertujuan untuk mencapai efek ini, mengubah kesadaran pembeli atau pemakainya, dan dengan demikian, menyebarkan benih-benih otonomi lebih jauh.

2.2 Pascakonspirasi sebagai Modalitas Operasional

Jika T.A.Z. menyediakan doktrin strategis, maka "Pascakonspirasi" karya Itjang Djoedibarie menyediakan etos operasional sehari-hari. Teks ini, dengan nadanya yang tajam dan personal, menawarkan kerangka kerja untuk berinteraksi yang menolak ilusi solidaritas kelompok dan merangkul realitas kepentingan individu yang terdesentralisasi.

2.2.1 Penolakan Struktur Formal

Djoedibarie secara eksplisit menolak "organisasi, jaringan, federasi, pertemuan mingguan, konsensus, dan semua sampah itu". Baginya, "Dari struktur tumbuh administrasi. Dari administrasi, pengkhianatan lahir." Penolakan ini lahir dari pengalaman pahit, tetapi menghasilkan prinsip operasional yang kuat: Egregore tidak boleh menjadi sebuah organisasi. Tidak ada keanggotaan formal, tidak ada pertemuan wajib, tidak ada komite. Semua interaksi harus bersifat ad hoc, berbasis proyek, dan diatur oleh protokol yang disepakati, bukan oleh birokrasi. Ini secara

langsung menginformasikan desain sistem tata kelola di Bab 5, yang harus bersifat *emergent* dan algoritmik, bukan prosedural dan manusiawi.

Skeptisisme radikal Djoedibarie terhadap kepercayaan interpersonal menemukan solusinya dalam teknologi yang diadopsi oleh *Egregore*. Sistem yang dibangun di atas *blockchain* dan *smart contract* pada dasarnya bersifat *trustless* (tanpa kepercayaan/tidak butuh kepercayaan). Aturan-aturan ekonomi dan tata kelola dieksekusi oleh kode yang tidak dapat diubah dan dapat diaudit secara publik, **bukan oleh niat baik individu yang bisa goyah.** Para konspirator tidak perlu saling percaya secara mutlak; mereka hanya perlu percaya pada validitas protokol. Dengan cara ini, teknologi desentralisasi menjadi manifestasi teknis dari filosofi Pascakonspirasi, menyelesaikan kontradiksi antara kebutuhan akan koordinasi yang kompleks dan penolakan terhadap struktur yang bergantung pada kepercayaan manusia.

2.2.2 Identitas Konspirator

Istilah "konspirator" diadopsi secara formal dalam *whitepaper* ini, mengikuti logika Djoedibarie. Dalam pandangan hukum negara, semua orang yang terlibat dalam rantai tindakan ilegal—mulai dari yang mencetak buku bajakan, yang menjualnya, hingga yang membacanya—adalah "konspirator". *Egregore* merangkul label ini. Ia menghapus perbedaan peran yang kaku (produsen, distributor, konsumen) dan mengakui bahwa semua yang berpartisipasi dalam jaringan afinitas ini, dalam kapasitas apa pun, adalah konspirator dalam proyek bersama untuk menciptakan otonomi. Ini adalah identitas yang cair dan inklusif, yang didefinisikan oleh tindakan, **bukan oleh status formal.**

2.2.3 Egoisme dan Ilegalisme

Djoedibarie menulis dari perspektif egois yang kuat: "Pascakonspirasi... adalah tentang bagaimana Ego menemukan jalannya". Ini sangat penting untuk memastikan bahwa model Egregore menarik bagi semua spektrum pemikiran anarkis, termasuk individualis dan egois yang mungkin curiga terhadap proyek-proyek yang berbau kolektivisme. Sistem ini tidak menuntut pengorbanan individu untuk "kebaikan bersama" yang abstrak. Sebaliknya, ia dirancang agar partisipasi dalam *Egregore* secara langsung menguntungkan dan memberdayakan Ego masing-masing konspirator. Keuntungan ini bisa bersifat materi (surplus dari penjualan produk), psikis (kesenangan dalam berkreasi dan melawan), atau sosial (afinitas dengan konspirator lain). "Ilegalisme sebagai filosofi hidup" juga dirangkul, bukan sebagai tujuan itu sendiri, tetapi sebagai konsekuensi tak terhindarkan dari hidup secara otonom di dalam masyarakat yang mengkriminalisasi tindakan-tindakan kebebasan.

Dengan mensintesis T.A.Z. dan Pascakonspirasi, *Egregore Nomad-Cryptography* menjadi lebih dari sekadar sistem ekonomi. Ia menjadi sebuah mesin perang nomaden yang beroperasi melalui konspirasi afinitas, terus-menerus menciptakan dan melarutkan zona-zona otonomi untuk mengejar kebebasan dan intensifikasi kehidupan bagi para konspiratornya.

3 Arsitektur Ekonomi Mutualis

Arsitektur ekonomi *Egregore Nomad-Cryptography* dibangun di atas fondasi Mutualisme, sebuah aliran pemikiran anarkis yang dipelopori oleh Pierre-Joseph Proudhon. Tujuannya adalah untuk menciptakan sistem pertukaran dan produksi yang adil, resiprokal, dan bebas dari eksploitasi, yang menyeimbangkan otonomi individu dengan tanggung jawab bersama. Model ini menolak profit sebagai tujuan utama dan sebaliknya berfokus pada pemenuhan kebutuhan dan distribusi surplus yang adil di antara para kontributor.

3.1 Prinsip-Prinsip Inti Mutualis

Tiga prinsip utama dari pemikiran Proudhon menjadi pilar bagi model ekonomi ini:

1. **Kredit Tanpa Bunga (Kredit Mutual):** Permintaan inti dari para konspirator untuk menyediakan modal pinjaman tanpa keuntungan selaras sempurna dengan kritik Proudhon terhadap sistem perbankan tradisional. Proudhon berpendapat bahwa bunga adalah bentuk eksploitasi yang melanggengkan ketidaksetaraan. Sebagai gantinya, ia mengusulkan "Bank Rakyat" atau lembaga kredit mutual yang akan memberikan pinjaman tanpa bunga, atau hanya dengan biaya administrasi minimal, untuk memungkinkan para pekerja mengakses alat produksi. Dalam *Egregore*, fungsi ini dipenuhi pada awalnya oleh pinjaman antar-konspirator dan kemudian oleh Kas Afinitas. Setiap Rupiah yang dipinjamkan sebagai modal akan dikembalikan persis sejumlah itu setelah produk terjual, **tanpa ada riba atau keuntungan bagi pemodal.** Pemodal hanya akan menerima bagian dari surplus jika mereka juga berkontribusi dalam pengerjaan proyek, dan **bagian tersebut dihitung berdasarkan kontribusi kerja mereka, bukan modal mereka.**
2. **Kepemilikan sebagai Kepenguasaan (Possession vs. Property):** Proudhon membuat perbedaan krusial antara dua jenis kepemilikan. "Property" (properti) adalah kepemilikan yang bersifat eksploitatif, seperti tanah yang disewakan atau pabrik yang mempekerjakan buruh, di mana pemilik mendapatkan keuntungan pasif dari kerja orang lain. Inilah yang ia sebut sebagai "pencurian". Sebaliknya, "Possession" (kepenguasaan) adalah kepemilikan atas alat-alat yang digunakan seseorang untuk bekerja, seperti alat seorang pengrajin atau tanah yang digarap oleh petani itu sendiri. Dalam Egregore, prinsip ini diterapkan secara ketat. Alat-alat produksi, baik yang dimiliki secara sah maupun yang "dibajak" dari tempat kerja kapitalis, dianggap sebagai possession oleh para konspirator yang menggunakannya selama proyek berlangsung. Tidak ada klaim kepemilikan yang dapat digunakan untuk mengekstrak nilai dari kerja orang lain.
3. **Teori Nilai Kerja (Labor Theory of Value):** Meskipun merupakan konsep yang diperdebatkan, prinsip dasarnya—bahwa nilai suatu komoditas atau jasa harus bergantung pada jumlah kerja yang diperlukan untuk

memproduksinya—menjadi landasan bagi model distribusi surplus. Namun, Egregore memperluas definisi "kerja" melampaui sekadar jam kerja, seperti yang akan diuraikan di bawah ini.

3.2 Formula Alokasi Surplus Terdistribusi (FAST)

Untuk memastikan pembagian surplus yang adil dan transparan, sebuah model matematis yang kuat diperlukan. Model ini, yang disebut Formula Alokasi Surplus Terdistribusi (FAST), mengadaptasi dan memperluas konsep pembagian hasil dari koperasi sambil mengintegrasikan teori keputusan modern untuk menangani kontribusi kualitatif.

3.2.1 Model Dasar: Adaptasi dari Sisa Hasil Usaha (SHU)

Model ini dimulai dengan mengadaptasi formula Sisa Hasil Usaha (SHU) yang digunakan dalam koperasi di Indonesia. Formula umum SHU untuk seorang anggota adalah:

$$SHU_{anggota} = JasaUsahaAnggota(JUA) + JasaModalAnggota(JMA)$$

Di mana JUA didasarkan pada partisipasi anggota dalam transaksi koperasi, dan JMA didasarkan pada simpanan modal anggota. Dalam model Egregore, prinsip kredit tanpa bunga secara efektif membuat [JMA] selalu bernilai nol. Oleh karena itu, formula disederhanakan menjadi:

$$Surplus_i = JasaKontribusi_i$$

Di mana $Surplus_i$ adalah bagian surplus yang diterima oleh $konspirator_i$. Dalam bentuk yang paling dasar, Jasa Kontribusi dapat dihitung secara proporsional:

$$JasaKontribusi_i = \frac{K_i}{\sum_{j=1}^{n} K_j} \times S_{total}$$

Di mana K_i adalah nilai total kontribusi konspirator i, $\sum_{j=1}^{n} K_j$ adalah jumlah total kontribusi dari semua n konspirator dalam proyek, dan S_{total} adalah total surplus bersih (pendapatan dikurangi biaya material) dari proyek tersebut. Tantangan utamanya adalah bagaimana mendefinisikan dan mengukur K_i secara adil.

3.2.2 Valuasi Kontribusi Multi-Atribut (VCMA)

Untuk mengatasi tantangan pengukuran kontribusi yang beragam (misalnya, menyablon, menulis, mendesain, mengoordinasi, mengambil risiko), model FAST mengadopsi kerangka kerja dari Teori Utilitas Multi-Atribut (MAUT) dan model penilaian berbobot (weighted scoring). MAUT adalah teknik analisis keputusan yang memungkinkan evaluasi opsi berdasarkan beberapa kriteria atau atribut, baik

kuantitatif maupun kualitatif. Ini memungkinkan kita untuk memecah konsep "kontribusi" yang abstrak menjadi komponen-komponen yang dapat dinilai.

Proses VCMA adalah sebagai berikut:

1. **Definisi Atribut Kontribusi**: Sebelum sebuah proyek dimulai, para konspirator yang terlibat secara konsensus mendefinisikan serangkaian atribut yang relevan untuk menilai kontribusi dalam proyek tersebut. Atribut-atribut ini dapat mencakup, tetapi tidak terbatas pada:
    - A_1: Waktu Kerja (Kuantitatif): Jam yang dihabiskan untuk tugas-tugas spesifik.
    - A_2: Kompleksitas Teknis (Kualitatif): Tingkat keahlian atau kesulitan teknis yang dibutuhkan.
    - A_3: Inisiatif & Kreativitas (Kualitatif): Kontribusi ide, desain, atau solusi inovatif.
    - A_4: Beban Emosional & Koordinasi (Kualitatif): Upaya dalam mengelola komunikasi, menyelesaikan konflik, atau menanggung stres proyek.
    - A_5: Pengambilan Risiko (Kualitatif): Paparan terhadap risiko fisik, hukum, atau finansial (misalnya, dalam tindakan pembajakan).
2. **Pembobotan Atribut** (W_j): Para konspirator kemudian menetapkan bobot persentase (W_j) untuk setiap atribut (A_j), yang mencerminkan tingkat kepentingannya untuk keberhasilan proyek tersebut. Total semua bobot harus sama dengan 1 (atau 100%). Misalnya, sebuah proyek desain mungkin memberikan bobot lebih tinggi pada A_3, sementara proyek pembajakan alat mungkin lebih tinggi pada A_5.

    $$\sum_{j=1}^{m} w_j = 1$$

    di mana m adalah jumlah atribut.
3. **Penilaian Atribut** (X_{ij}): Setiap konspirator i dinilai pada setiap atribut j. Untuk atribut kuantitatif seperti A_1, ini adalah pengukuran langsung (misalnya, 40 jam). Untuk atribut kualitatif (A_2 hingga A_5), penilaian ini dilakukan melalui Sistem Evaluasi Rekan (dibahas di 2.3) pada skala yang telah ditentukan (misalnya, 1-10).
4. **Normalisasi melalui Fungsi Utilitas** $U_j(x_{ij})$: Untuk membandingkan atribut yang berbeda skala, setiap skor mentah x_{ij} diubah menjadi skor utilitas pada skala standar (misalnya, 0-100) menggunakan fungsi utilitas. Untuk kesederhanaan, dapat digunakan normalisasi linier:

    $$U_j(x_{ij}) = 100 \times \frac{x_{ij} - x_{j,min}}{x_{j,max} - x_{j,min}}$$

    di mana $x_{j,min}$ dan $x_{j,max}$ adalah skor minimum dan maksimum yang mungkin untuk atribut j.

5. **Perhitungan Skor Kontribusi Total** (K_i): Skor kontribusi total untuk konspirator i adalah jumlah tertimbang dari skor utilitas mereka di semua atribut:

$$K_i = \sum_{j=1}^{m} \left(w_j \times U_j(x_{ij}) \right)$$

Model ini memberikan kerangka kerja yang fleksibel, transparan, dan dapat disesuaikan untuk menilai kontribusi secara holistik, melampaui sekadar perhitungan jam kerja.

3.2.3 Sistem Evaluasi Rekan (*Peer Evaluation System*)

Untuk atribut kualitatif, penilaian yang objektif sulit dicapai. Oleh karena itu, model ini mengandalkan sistem evaluasi rekan yang terstruktur, sebuah metode yang telah terbukti efektif dalam konteks pendidikan dan kerja tim. Setelah proyek selesai, setiap konspirator akan menilai kontribusi rekan-rekan mereka (dan diri mereka sendiri) pada setiap atribut kualitatif. Untuk menjaga kejujuran dan mengurangi bias, proses ini idealnya dilakukan secara anonim, sebuah fitur yang dapat difasilitasi oleh teknologi kriptografi seperti zk-SNARKs (lihat bagian 4.4).

Skor akhir untuk seorang individu pada atribut kualitatif adalah rata-rata dari semua penilaian yang diterima dari rekan-rekannya. Proses ini didukung oleh rubrik yang jelas yang mendefinisikan setiap tingkat skor (misalnya, apa arti skor '7' untuk 'Inisiatif & Kreativitas') untuk memastikan konsistensi.

Tabel 1: Contoh Matriks Penilaian Kontribusi Multi-Atribut (VCMA)

ID_Proyek	ID_Konspirator	Atribut Kontribusi (Aj)	Bobot (wj)	Skor Mentah (xij)	Skor Utilitas (Uj)	Skor Terbobot (wj×Uj)	Total Skor Kontribusi (Ki)
P001	Konspirator A	Waktu Kerja (A1)	0.4	40 jam	100	40	70.5
		Kompleksitas Teknis (A2)	0.2	10-Aug	75	15	
		Inisiatif & Kreativitas (A3)	0.3	10-May	40	12	
		Pengambilan Risiko (A5)	0.1	10-Apr	35	3.5	

P001	Konspirator B	Waktu Kerja (A1)	0.4	25 jam	50	20	62
		Kompleksitas Teknis (A2)	0.2	10-Jun	50	10	
		Inisiatif & Kreativitas (A3)	0.3	10-Sep	90	27	
		Pengambilan Risiko (A5)	0.1	10-May	50	5	
P001	Konspirator C	Waktu Kerja (A1)	0.4	15 jam	25	10	52.5
		Kompleksitas Teknis (A2)	0.2	10-May	37.5	7.5	
		Inisiatif & Kreativitas (A3)	0.3	10-Jun	50	15	
		Pengambilan Risiko (A5)	0.1	10-Oct	100	20	

Catatan: Skor Utilitas untuk atribut kualitatif dihitung berdasarkan evaluasi rekan. Total skor kontribusi (K_i) kemudian digunakan dalam formula alokasi surplus.

3.3 Mekanisme Kas Afinitas

Untuk memastikan keberlanjutan dan kemandirian *Egregore* dalam jangka panjang, sebuah Kas Afinitas dibentuk. Mekanismenya sederhana: 5% dari surplus pribadi setiap konspirator ($Surplus_i$) dari setiap proyek yang berhasil secara otomatis dipotong dan disalurkan ke dalam perbendaharaan bersama ini. Dana ini tidak dimiliki oleh individu mana pun, melainkan oleh *Egregore* itu sendiri, dan pengelolaannya diatur oleh protokol tata kelola yang terdesentralisasi (Bab 5).

Tujuan utama dari Kas Afinitas adalah:

1. **Modal Mandiri**: Menyediakan modal awal untuk proyek-proyek di masa depan, yang secara bertahap akan mengurangi dan akhirnya menghilangkan ketergantungan pada pinjaman dari individu. Ini adalah langkah krusial untuk mencapai otonomi finansial penuh.

2. **Biaya Operasional**: Menutupi biaya-biaya bersama yang mungkin timbul, seperti biaya hosting untuk platform digital, sewa ruang kerja temporer, atau biaya transaksi di *blockchain*.
3. **Dana Darurat**: Berfungsi sebagai jaring pengaman, yang dapat digunakan untuk membantu konspirator yang menghadapi kesulitan tak terduga, sesuai dengan keputusan konsensus.

Dengan arsitektur ekonomi ini, *Egregore Nomad-Cryptography* menciptakan sebuah siklus nilai yang mandiri: produksi menghasilkan surplus, surplus didistribusikan secara adil berdasarkan kontribusi yang dinilai secara holistik, dan sebagian kecil dari surplus tersebut diinvestasikan kembali untuk memperkuat otonomi kolektif di masa depan.

4 Infrastruktur Keuangan Terdesentralisasi (DeFi)

Untuk mewujudkan prinsip-prinsip otonomi, privasi, dan penolakan terhadap kontrol negara, *Egregore Nomad-Cryptography* harus dibangun di atas fondasi teknologi yang sejalan dengan etosnya. Keuangan Terdesentralisasi (DeFi) menawarkan tumpukan teknologi yang diperlukan untuk menciptakan sistem keuangan yang transparan, tahan sensor, dan dapat diprogram tanpa memerlukan perantara terpusat seperti bank atau lembaga keuangan negara.

4.1 Protokol Perbendaharaan On-Chain

Kas Afinitas, yang dijelaskan di Bab 3, tidak akan disimpan dalam rekening bank atau dipegang oleh seorang bendahara. Sebaliknya, ia akan diimplementasikan sebagai *smart contract* (kontrak pintar) di atas sebuah *blockchain* publik, seperti Ethereum atau jaringan Lapisan-2 (Layer-2) yang menawarkan biaya lebih rendah. Pendekatan ini mengubah Kas Afinitas menjadi sebuah Perbendaharaan On-Chain dengan karakteristik sebagai berikut:

- **Transparansi Radikal**: Setiap transaksi yang masuk dan keluar dari kas tercatat secara permanen dan dapat diaudit oleh siapa saja secara publik di *blockchain*. Ini menghilangkan kemungkinan penyalahgunaan dana atau kurangnya transparansi keuangan.
- **Tahan Sensor**: Karena perbendaharaan ada di jaringan terdesentralisasi global, tidak ada entitas tunggal—baik itu bank maupun negara—yang dapat membekukan, menyita, atau mengontrol dana tersebut. Ini adalah perwujudan teknis dari otonomi finansial.
- **Otomatisasi**: Otomisasi mengatur kas, seperti pemotongan 5% dari surplus proyek atau pengeluaran dana berdasarkan keputusan tata kelola, dapat dikodekan langsung ke dalam smart contract. Ini memastikan bahwa aturan ditegakkan secara otomatis dan tanpa bias, mengurangi kebutuhan akan administrasi manual dan potensi kesalahan manusia.

Secara esensial, Perbendaharaan *On-Chain* ini berfungsi dalam skala mikro, di mana operasinya diatur oleh kode yang disepakati bersama, bukan oleh hierarki manajemen.

4.2 Analisis Komparatif Aset Digital

Pemilihan aset digital untuk menyimpan nilai di dalam Kas Afinitas adalah keputusan strategis yang melibatkan pertukaran antara stabilitas dan privasi. Dua kategori utama dipertimbangkan, sejalan dengan permintaan untuk mengeksplorasi alternatif selain BIDR.

4.2.1 Opsi 1: Stablecoin Terdesentralisasi (misalnya, DAI)

Stablecoin adalah aset kripto yang dirancang untuk mempertahankan nilai yang stabil dengan mematoknya ke aset lain, biasanya mata uang fiat seperti Dolar AS.

Keunggulan:

- Stabilitas: Nilai yang stabil (sekitar $1.00 USD) membuat stablecoin sangat berguna sebagai unit hitung dan penyimpan nilai jangka pendek. Ini menyederhanakan akuntansi, penetapan harga produk, dan perencanaan keuangan.
- Desentralisasi (khusus DAI): Tidak seperti stablecoin terpusat seperti Tether (USDT) atau USD Coin (USDC) yang didukung oleh aset di rekening bank, DAI adalah stablecoin terdesentralisasi. Nilainya dipertahankan melalui sistem agunan kripto yang terkunci dalam smart contract di platform MakerDAO, yang dikelola oleh sebuah DAO. Ini membuatnya lebih tahan terhadap sensor dan risiko kustodian tunggal.

Kelemahan:

- Kurangnya Privasi: Transaksi DAI di *blockchain* Ethereum bersifat pseudonim tetapi sepenuhnya transparan. Alamat pengirim, penerima, dan jumlah transaksi dapat dilihat oleh siapa saja, yang bertentangan dengan kebutuhan OPSEC dan etos "invisibilitas".
- Ketergantungan Fiat: Meskipun terdesentralisasi, nilainya tetap dipatok pada Dolar AS, yang berarti ia masih terikat secara tidak langsung pada sistem keuangan negara yang ingin dihindari.

4.2.2 Opsi 2: Kripto Privat (misalnya, Monero/XMR)

Kripto privat dirancang secara khusus untuk mengaburkan detail transaksi, memberikan anonimitas yang kuat bagi penggunanya.

Keunggulan:

- Privasi Superior: Monero menggunakan kombinasi kriptografi canggih—ring signatures, stealth addresses, dan RingCT—untuk menyembunyikan pengirim, penerima, dan jumlah setiap transaksi. Ini menjadikannya hampir tidak dapat dilacak, selaras sempurna dengan kebutuhan akan "invisibilitas" TAZ dan keamanan operasional yang ketat.

- Desentralisasi Penuh: Monero adalah proyek open-source yang digerakkan oleh komunitas tanpa entitas pusat, menjadikannya sangat tahan sensor dan selaras dengan prinsip-prinsip anarkis.

Kelemahan:

- Volatilitas Tinggi: Seperti Bitcoin, harga Monero sangat fluktuatif. Menggunakannya sebagai unit utama untuk kas akan membuat perencanaan keuangan menjadi sangat sulit dan berisiko.

4.2.3 Rekomendasi Strategi Hibrida

Mengingat kelebihan dan kekurangan masing-masing, strategi yang paling bijaksana adalah pendekatan hibrida:

1. Kas Operasional: Sebagian besar Kas Afinitas (misalnya, 80-90%) disimpan dalam stablecoin terdesentralisasi seperti DAI. Ini memberikan stabilitas yang diperlukan untuk operasi sehari-hari, penggantian modal, dan perhitungan surplus.
2. Kas Privasi/Strategis: Sebagian kecil kas (misalnya, 10-20%) dialokasikan ke kripto privat seperti Monero. Dana ini digunakan untuk transaksi yang memerlukan anonimitas absolut atau sebagai lindung nilai jangka panjang terhadap devaluasi mata uang fiat.

Keputusan mengenai rasio alokasi antara DAI dan Monero dapat menjadi salah satu agenda dalam proses tata kelola, yang memungkinkan *Egregore* untuk menyesuaikan strateginya seiring waktu.

4.3 Akuisisi Aset Peer-to-Peer (P2P)

Untuk menjaga anonimitas dan menghindari yurisdiksi negara, Egregore harus menolak penggunaan bursa kripto terpusat (CEX) seperti Indodax atau Binance. Bursa-bursa ini tunduk pada peraturan Know Your Customer (KYC), yang mengharuskan pengguna untuk menyerahkan identitas mereka, menciptakan titik kerentanan yang signifikan. Sebagai gantinya, akuisisi aset kripto harus dilakukan melalui platform peer-to-peer (P2P) terdesentralisasi.

Bisq adalah contoh utama dari platform semacam ini. Bisq adalah perangkat lunak desktop open-source yang menghubungkan pengguna secara langsung dalam jaringan P2P yang dibangun di atas Tor untuk privasi maksimal. Cara kerjanya adalah sebagai berikut:

- Tanpa Registrasi: Tidak ada akun, tidak ada verifikasi identitas. Pengguna cukup mengunduh dan menjalankan perangkat lunak.
- Non-Kustodian: Bisq tidak pernah memegang dana pengguna. Bitcoin yang diperdagangkan dikunci dalam alamat multisignature 2-dari-2 yang dikendalikan bersama oleh pembeli dan penjual. Pembayaran fiat (misalnya, transfer bank, e-wallet) terjadi langsung di antara para pihak.
- Keamanan: Deposit keamanan dalam bentuk Bitcoin diperlukan dari kedua belah pihak untuk mencegah penipuan. Jika terjadi sengketa, sistem arbitrase terdesentralisasi akan menyelesaikannya.

- Privasi: Semua komunikasi dienkripsi ujung-ke-ujung dan dirutekan melalui jaringan Tor.

Platform seperti Bisq (atau alternatifnya untuk Monero, seperti yang pernah ditawarkan oleh LocalMonero) memungkinkan konspirator untuk mengubah Rupiah (IDR) menjadi aset digital yang dibutuhkan (BTC, lalu menukarnya dengan DAI atau XMR) secara langsung dengan individu lain, meminimalkan jejak dan menghindari pengawasan terpusat.

4.4 Kriptografi Lanjutan: Verifikasi Privat dengan zk-SNARKs

Untuk mencapai tingkat privasi dan keamanan tertinggi, Egregore dapat mengintegrasikan salah satu teknologi kriptografi paling canggih: zk-SNARKs.

4.4.1 Pengenalan Konseptual

Zero-Knowledge Proofs (ZKP) adalah protokol kriptografi di mana satu pihak (Prover) dapat membuktikan kepada pihak lain (Verifier) bahwa mereka mengetahui suatu nilai atau bahwa suatu pernyataan itu benar, tanpa mengungkapkan informasi apa pun selain fakta bahwa pernyataan itu benar. Analogi klasiknya adalah "Gua Ali Baba", di mana Prover membuktikan bahwa dia tahu kata sandi rahasia untuk membuka pintu di dalam gua tanpa pernah mengucapkan kata sandi itu sendiri.

zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) adalah jenis ZKP yang sangat efisien.

- Zero-Knowledge: Verifier tidak mempelajari apa pun tentang informasi rahasia (witness).
- Succinct: Bukti (proof) yang dihasilkan sangat kecil dan cepat untuk diverifikasi, bahkan jika komputasi yang dibuktikan sangat kompleks.
- Non-Interactive: Prover dapat menghasilkan bukti yang dapat diverifikasi oleh siapa saja, kapan saja, tanpa memerlukan interaksi bolak-balik.
- Argument of Knowledge: Prover tidak dapat membuat bukti yang valid tanpa benar-benar mengetahui informasi rahasia tersebut.

Secara teknis, zk-SNARKs bekerja dengan mengubah program komputasi menjadi representasi matematis (seperti Quadratic Arithmetic Program), yang kemudian dievaluasi pada titik acak rahasia menggunakan enkripsi homomorfik. Proses ini memerlukan fase "trusted setup" untuk menghasilkan kunci pembuktian (proving key) dan kunci verifikasi (verification key). Siapa pun yang mengetahui parameter rahasia dari setup ini ("toxic waste") dapat membuat bukti palsu, sehingga proses ini harus dilakukan dengan sangat hati-hati.

4.4.2 Aplikasi dalam Egregore

Dalam konteks Egregore, zk-SNARKs memungkinkan dua aplikasi revolusioner:

1. **Verifikasi Kontribusi Anonim**: Dalam Sistem Evaluasi Rekan (Bab 3.2.3), anonimitas sangat penting. Menggunakan zk-SNARKs, seorang konspirator dapat mengirimkan penilaian mereka ke smart contract tata kelola bersama dengan sebuah bukti. Bukti ini akan memverifikasi bahwa: (a) pengirim adalah konspirator yang sah dalam proyek tersebut, dan (b)

mereka belum mengirimkan penilaian sebelumnya, semua tanpa mengungkapkan alamat blockchain mereka. Ini memungkinkan pencatatan kontribusi kualitatif secara trustless dan terdesentralisasi sambil menjaga anonimitas operasional penuh.

2. **Audit Kas Privat dan Transaksi Rahasia**: Egregore dapat menggunakan zk-SNARKs untuk menciptakan sistem transaksi rahasia di atas blockchain publik, mirip dengan cara kerja Zcash.

Kas Afinitas dapat membuktikan secara publik bahwa ia memiliki dana yang cukup untuk membiayai sebuah proyek (Proof of Reserves) tanpa mengungkapkan total saldo atau riwayat transaksinya. Demikian pula, pembayaran surplus kepada konspirator dapat dilakukan secara rahasia, di mana hanya validitas transaksi yang diverifikasi di blockchain, sementara detail pengirim, penerima, dan jumlah tetap tersembunyi. Ini adalah sintesis sempurna antara transparansi (validitas terjamin) dan privasi (detail tersembunyi).

Integrasi infrastruktur DeFi ini mengubah Egregore dari sekadar konsep ekonomi alternatif menjadi entitas operasional yang tangguh, otonom, dan mampu beroperasi di luar jangkauan sistem kontrol tradisional.

5.0 Tata Kelola Emergen: Konsensus Berbasis Reputasi

Sistem tata kelola *Egregore Nomad-Cryptography* dirancang untuk menolak secara fundamental model-model yang mereplikasi struktur negara, terutama demokrasi perwakilan dan pemungutan suara mayoritas. Tujuannya adalah untuk menciptakan proses pengambilan keputusan yang sepenuhnya terdesentralisasi, egaliter, dan berbasis konsensus, di mana pengaruh diperoleh melalui kontribusi, bukan melalui kekuasaan atau modal.

5.1 Melampaui Voting: Kritik terhadap Tirani Mayoritas

Permintaan untuk menolak sistem voting adalah inti dari desain tata kelola ini. Dari perspektif anarkis, pemungutan suara (voting) bukanlah alat pembebasan, melainkan mekanisme untuk mengelola konflik dan memaksakan kehendak mayoritas atas minoritas. Proses ini secara inheren menciptakan dinamika pemenang-kalah, yang memecah belah dan menghasilkan "mayoritas yang puas dan minoritas yang tidak puas". Ini adalah tirani mayoritas, sebuah bentuk despotisme dari orang banyak yang sama menindasnya dengan despotisme satu orang. Seperti yang diamati Murray Bookchin, bahkan dalam proses konsensus, tekanan psikologis dapat digunakan untuk memaksa minoritas agar tidak menyuarakan penolakan, yang merupakan bentuk otoritarianisme terselubung. Oleh karena itu, Egregore harus mencari alternatif yang benar-benar menghormati otonomi setiap individu dan bertujuan untuk sintesis, bukan dominasi.

5.2 Model Konsensus Formal

Sebagai alternatif dari voting, Egregore mengadopsi model konsensus formal. Ini adalah proses pengambilan keputusan yang terstruktur di mana sebuah kelompok berusaha mencapai kesepakatan yang dapat diterima oleh semua anggota, bahkan

jika beberapa tidak sepenuhnya antusias. Tujuannya bukan unanimitas (semua orang sangat setuju), melainkan consent (tidak ada yang secara fundamental menentang).

Proses ini umumnya mengikuti langkah-langkah berikut:

1. **Diskusi dan Presentasi Proposal**: Sebuah isu atau proposal diperkenalkan dan didiskusikan secara terbuka. Tujuannya adalah untuk berbagi informasi, mengklarifikasi pertanyaan, dan memahami semua sudut pandang.
2. **Identifikasi Keprihatinan**: Fasilitator (peran yang dapat dipegang secara bergilir) membimbing diskusi untuk mengidentifikasi setiap keprihatinan, keraguan, atau potensi masalah terkait proposal.
3. **Modifikasi Proposal**: Proposal dimodifikasi dan disempurnakan secara kolaboratif untuk mencoba mengakomodasi semua keprihatinan yang muncul.
4. **Panggilan untuk Konsensus**: Setelah proposal dianggap matang, fasilitator secara formal "memanggil konsensus". Setiap konspirator yang terlibat kemudian menyatakan posisi mereka. Posisi yang umum adalah:
    - **Setuju (Agree)**: Mendukung proposal.
    - **Berdiri di Samping (Stand Aside)**: Memiliki keberatan kecil atau tidak sepenuhnya setuju, tetapi tidak akan menghalangi kelompok untuk maju. Ini bukan "ya" yang antusias, tetapi sebuah pernyataan "Saya bisa hidup dengan ini."
    - **Memblokir (Block)**: Memiliki keberatan fundamental yang serius terhadap proposal, biasanya karena melanggar prinsip inti atau nilai-nilai *Egregore*. Sebuah blok adalah pernyataan "Saya tidak bisa membiarkan kelompok membuat keputusan ini."
5. **Penyelesaian**: Sebuah proposal dianggap mencapai konsensus jika tidak ada yang memblokir. Jika ada satu atau lebih blok, kelompok harus kembali ke tahap diskusi untuk memahami keberatan tersebut dan mencoba menemukan solusi yang dapat diterima oleh semua pihak. Sebuah blok tidak dilihat sebagai tindakan negatif, melainkan sebagai informasi penting bahwa proposal tersebut memiliki cacat serius yang perlu diperbaiki.

Untuk memfasilitasi proses ini dalam kelompok, terutama yang lebih besar, metode non-verbal seperti sinyal tangan (hand signals) dapat digunakan untuk mengukur "suhu" ruangan dengan cepat tanpa menginterupsi pembicara.

5.3 Sistem Reputasi Dinamis (SRD)

Meskipun konsensus formal menyediakan proses yang egaliter, ia bisa menjadi tidak efisien jika semua pendapat dianggap memiliki bobot yang sama terlepas dari pengalaman, keahlian, atau tingkat keterlibatan. Untuk mengatasi ini tanpa kembali ke hierarki formal, *Egregore* mengimplementasikan Sistem Reputasi Dinamis (SRD). Model ini terinspirasi oleh DAO berbasis reputasi seperti Colony,

di mana pengaruh dalam tata kelola diperoleh melalui kontribusi yang terbukti, bukan melalui kepemilikan token.

5.3.1 Perhitungan dan Peluruhan Reputasi

- **Perolehan Reputasi**: Skor reputasi (R_i) untuk setiap konspirator i dihitung secara langsung dari kontribusi mereka yang telah divalidasi. Setiap kali seorang konspirator menyelesaikan sebuah proyek, skor kontribusi total mereka (K_i dari model VCMA di bagian 3.2.2) ditambahkan ke skor reputasi kumulatif mereka.

$$R_{i,baru} = R_{i,lama} + K_{i,proyek}$$

  Reputasi adalah skor non-transferable yang terikat pada identitas digital konspirator. Ia tidak dapat dibeli, dijual, atau didelegasikan seperti token tata kelola, yang secara efektif mencegah plutokrasi (pemerintahan oleh orang kaya).
- **Peluruhan Reputasi (Reputation Decay)**: Untuk memastikan bahwa pengaruh mencerminkan partisipasi yang aktif dan relevan, reputasi akan meluruh seiring berjalannya waktu. Ini mencegah konspirator yang sudah lama tidak aktif untuk mempertahankan pengaruh yang tidak semestinya. Fungsi peluruhan eksponensial digunakan untuk memodelkan ini, di mana reputasi berkurang secara terus-menerus pada tingkat yang proporsional dengan nilainya saat ini.

$$R_i(t) = R_{i,0} \times e^{-\lambda t}$$

  Di mana:
  - $R_i(t)$ adalah reputasi konspirator i pada waktu t.
  - $R_{i,0}$ adalah reputasi pada waktu awal (setelah kontribusi terakhir).
  - λ (lambda) adalah konstanta peluruhan, sebuah parameter sistem yang menentukan seberapa cepat reputasi memudar.
  - t adalah waktu yang telah berlalu sejak kontribusi terakhir.

  Mekanisme peluruhan ini menciptakan insentif untuk partisipasi berkelanjutan; untuk mempertahankan pengaruh, seseorang harus terus berkontribusi.

5.3.2 Reputasi sebagai Bobot, Bukan Suara

Ini adalah inovasi krusial dalam model tata kelola *Egregore*. Tidak seperti banyak DAO, skor reputasi tidak digunakan sebagai bobot suara dalam sistem voting (karena voting itu sendiri ditolak). Sebaliknya, reputasi berfungsi sebagai bobot pengaruh sosial yang transparan dan dapat diverifikasi dalam proses konsensus.

Dalam praktiknya, ini berarti:

- **Sinyal Keahlian:** Ketika sebuah proposal didiskusikan, pendapat dari seorang konspirator dengan reputasi tinggi di bidang yang relevan

(misalnya, reputasi tinggi dalam desain untuk proposal tentang estetika produk) secara alami akan diberi bobot lebih oleh para partisipan lain. Reputasi menjadi penanda publik untuk keahlian dan komitmen masa lalu.
- **Tanpa Kekuasaan:** Meskipun pendapat mereka memiliki bobot sosial yang lebih besar, konspirator dengan reputasi tinggi tetap tidak memiliki kekuatan formal untuk memaksakan keputusan. Mereka masih harus meyakinkan yang lain melalui argumen dan proses konsensus. Mereka tidak dapat "mengalahkan" sebuah blok hanya karena reputasi mereka tinggi.

Sistem ini menciptakan meritokrasi yang cair. Ia memungkinkan individu yang paling kompeten dan berdedikasi untuk memandu diskusi dan mempercepat pengambilan keputusan yang baik, tanpa melanggar prinsip otonomi individu atau kesetaraan fundamental. Ini adalah sistem yang bahkan dapat diterima oleh seorang egois, karena pengaruh yang mereka peroleh adalah cerminan langsung dari manifestasi kemampuan dan usaha mereka, bukan dari posisi atau kekayaan.

5.3.3 Evolusi Potensial

Sebagai jalur evolusi potensial di masa depan, konspirator, dalam model ini, dapat secara temporer "mendelegasikan" pengaruh mereka pada topik tertentu kepada konspirator lain yang mereka anggap lebih ahli. Misalnya, seorang penulis dapat mendelegasikan pengaruhnya pada keputusan teknis tentang *smart contract* kepada seorang programmer yang mereka percayai. Delegasi ini bersifat cair, artinya dapat ditarik kembali kapan saja. Ini memungkinkan spesialisasi yang lebih dalam dalam pengambilan keputusan tanpa menciptakan perwakilan tetap, sehingga dapat menutup kebobrokan antara demokrasi langsung dan perwakilan ahli.

Tata kelola emergen ini, yang menggabungkan proses konsensus formal dengan sistem reputasi dinamis, menawarkan solusi yang kuat untuk tantangan koordinasi dalam kelompok anarkis. Ia menolak mekanisme negara sambil membangun sistem yang meritokratis, adaptif, dan tangguh.

6.0 Integrasi Agen Ekonomi Otonom (AEA)

Untuk meningkatkan efisiensi, mengotomatiskan tugas-tugas repetitif, dan memperkuat desentralisasi, *Egregore Nomad-Cryptography* mengintegrasikan konsep Agen Ekonomi Otonom (AEA). AEA adalah entitas perangkat lunak cerdas yang bertindak secara otonom atas nama pemiliknya (dalam hal ini, para konspirator atau Egregore itu sendiri) untuk mencapai tujuan ekonomi tertentu dengan intervensi manusia yang minimal atau tanpa intervensi sama sekali. Dalam ekosistem ini, AEA berfungsi sebagai perpanjangan digital dari kehendak para konspirator, menangani tugas-tugas administratif dan operasional sehingga para konspirator dapat fokus pada kerja kreatif dan strategis.

6.1 Arsitektur dan Kerangka Kerja AEA

Arsitektur sistem AEA untuk Egregore dirancang agar modular, dapat diskalakan, dan selaras dengan prinsip desentralisasi.

6.1.1 Arsitektur Multi-Agen: Orchestrator-Worker

Mengingat keragaman tugas dalam *Egregore* (dari manajemen keuangan hingga pemantauan pasar), arsitektur multi-agen lebih cocok daripada agen tunggal monolitik. Pola arsitektur yang diadopsi adalah *Orchestrator-Worker* yang digerakkan oleh peristiwa (event-driven), sebuah pola yang sangat efektif untuk sistem terdistribusi.

- **Agent Supervisor (Orchestrator)**: Ini adalah agen tingkat tinggi yang berfungsi sebagai koordinator utama. Ia menerima tujuan umum (misalnya, "Luncurkan proyek zine baru"), memecahnya menjadi sub-tugas yang dapat ditindaklanjuti, dan mendelegasikannya ke agen-agen spesialis yang sesuai. Ia memantau kemajuan keseluruhan dan mengintegrasikan hasil dari para pekerja.
- **Agent Worker (Specialist)**: Ini adalah agen-agen yang lebih kecil dengan fungsi yang sangat spesifik dan terdefinisi dengan baik. Mereka beroperasi secara independen untuk menyelesaikan tugas yang didelegasikan oleh Supervisor. Contohnya termasuk Agen Perbendaharaan, Agen Pasar, atau Agen Kalkulasi Kontribusi.

Pola ini memungkinkan spesialisasi dan modularitas. Setiap agen dapat dikembangkan, diuji, dan diperbarui secara independen, membuat keseluruhan sistem lebih kuat dan lebih mudah dikelola.

6.1.2 Kerangka Kerja Teknis dan Implementasi

Implementasi AEA ini tidak dimulai dari nol. Ia akan dibangun di atas kerangka kerja open-source yang sudah ada, yang menyediakan fondasi untuk pengembangan agen.

- Fetch.ai AEA Framework: Kerangka kerja ini, yang ditulis terutama dalam Python, secara eksplisit dirancang untuk membangun Agen Ekonomi Otonom. Ia menyediakan alat untuk membuat agen, mendefinisikan keterampilan (skills), protokol komunikasi, dan koneksi ke jaringan terdesentralisasi dan blockchain. Repositori GitHub-nya (fetchai/agents-aea) berfungsi sebagai titik awal utama untuk pengembangan.
- Repositori Terkait: Ekosistem agen AI yang lebih luas menyediakan banyak contoh dan perangkat yang dapat diadaptasi, seperti evolving-agents untuk sistem agen yang dapat beradaptasi dan autonomys-agents yang menunjukkan integrasi dengan blockchain dan manajemen pengalaman agen. Referensi ke proyek-proyek ini menunjukkan bahwa teknologi yang diusulkan didasarkan pada praktik pengembangan yang aktif dan nyata.

6.2 Protokol Komunikasi dan Peran Agen

Agar dapat berkolaborasi secara efektif, para agen dalam arsitektur multi-agen memerlukan bahasa dan protokol komunikasi yang standar.

6.2.1 Bahasa Komunikasi Agen (ACL)

Komunikasi antar-agen akan didasarkan pada standar FIPA-ACL (Foundation for Intelligent Physical Agents-Agent Communication Language). FIPA-ACL didasarkan pada teori tindak tutur (speech act theory), di mana setiap pesan bukan hanya transmisi data, tetapi sebuah tindakan komunikatif yang memiliki niat dan tujuan tertentu.

Struktur pesan FIPA-ACL yang mendasar mencakup beberapa parameter kunci:

- [:performative]: Tindakan komunikatif yang dilakukan (parameter wajib). Contohnya termasuk [REQUEST] (meminta agen lain melakukan suatu tindakan), INFORM (memberikan informasi), [PROPOSE] (mengajukan proposal), [ACCEPT_PROPOSAL], [REJECT_PROPOSAL].
- [:sender]: Pengirim pesan.
- [:receiver]: Penerima pesan.
- [:content]: Isi sebenarnya dari pesan.
- [:language]: Bahasa yang digunakan untuk mengkodekan konten (misalnya, SL).
- [:ontology]: Ontologi yang mendefinisikan makna istilah dalam konten.
- [:conversation-id]: Pengidentifikasi unik untuk melacak alur percakapan.

Penggunaan protokol standar seperti [FIPA-ACL], yang implementasinya dapat ditemukan di repositori seperti sarl-acl , memastikan interoperabilitas dan komunikasi yang jelas antar agen, bahkan jika mereka dikembangkan secara terpisah.

6.2.2 Peran dan Fungsi Agen dalam Egregore

Tabel berikut menguraikan peran dan fungsi spesifik dari berbagai AEA yang diusulkan untuk beroperasi dalam ekosistem *Egregore Nomad-Cryptography*.

Tabel 2: Peran dan Fungsi Agen dalam Ekosistem Egregore

Nama Agen	Tipe Agen	Fungsi Utama	Alat/Protokol yang Digunakan	Pemicu (Trigger)
Egregore Supervisor	Supervisor	- Menerima tujuan proyek baru dari konspirator. - Memecah tujuan menjadi sub-tugas (misalnya, alokasi modal, produksi, distribusi, perhitungan surplus). - Mendelegasikan sub-tugas ke Agen Worker yang sesuai. - Memantau status proyek dan mengagregasi laporan.	FIPA-ACL (REQUEST, INFORM), Logika Perencanaan Internal	Input manual dari konspirator melalui antarmuka yang aman.

Agen Perbendaharaan	Worker	- Memantau saldo Kas Afinitas secara real-time. - Mengeksekusi permintaan modal untuk proyek baru setelah disetujui oleh tata kelola. - Secara otomatis mengeksekusi potongan 5% dari surplus yang masuk. - Memberikan notifikasi jika saldo kas di bawah ambang batas tertentu.	Interaksi Smart Contract (Web3.py), API Oracle Harga, FIPA-ACL (INFORM)	Permintaan dari Supervisor, transaksi masuk ke alamat kas.
Agen Pasar P2P	Worker	- Memantau penawaran beli/jual di bursa P2P (misalnya, Bisq API) untuk aset yang relevan (BTC, XMR, DAI). - Memberi tahu konspirator tentang peluang arbitrase atau harga yang menguntungkan. - (Potensi di masa depan) Secara otonom mengeksekusi perdagangan kecil berdasarkan parameter yang telah ditentukan.	API Bursa P2P, FIPA-ACL (INFORM)	Pemicu berbasis waktu (misalnya, setiap jam), perubahan harga yang signifikan.
Agen Kalkulasi Kontribusi	Worker	- Mengumpulkan data kontribusi kuantitatif (misalnya, log waktu) dan hasil evaluasi rekan anonim. - Menerapkan model VCMA (Bab 3.2.2) untuk menghitung skor kontribusi total (Ki) untuk setiap konspirator. - Menghitung alokasi surplus akhir untuk setiap konspirator.	FIPA-ACL (REQUEST data), Logika Matematis Internal (MAUT)	Sinyal "Proyek Selesai" dari Supervisor.

Agen Tata Kelola	Worker	- Mencatat proposal baru ke sistem tata kelola. - Menghitung skor reputasi dinamis (Ri) dan menerapkan fungsi peluruhan. - Memberikan data reputasi yang relevan selama diskusi konsensus. - Secara anonim mengagregasi dan mempublikasikan hasil evaluasi rekan.	Interaksi Smart Contract, zk-SNARK verifier, FIPA-ACL (INFORM)	Pengajuan proposal baru, penyelesaian proyek.

Integrasi AEA mengubah Egregore menjadi sistem sosio-teknis hibrida. Ini mengotomatiskan kerja-kerja yang membosankan dan rawan kesalahan, memungkinkan para konspirator untuk memfokuskan energi mereka pada esensi dari eksperimen ini: penciptaan, kolaborasi, dan penemuan bentuk-bentuk baru kehidupan otonom.

7.0 Panduan Operasional: Sabotase, Pembajakan, dan Keamanan

Eksperimen *Egregore Nomad-Cryptography* beroperasi di dalam dan melawan lingkungan yang seringkali memusuhi. Negara dan struktur kapitalis memiliki kepentingan untuk mempertahankan status quo dan akan menggunakan aparatus pengawasan dan penegakan hukumnya untuk menekan aktivitas yang mengancamnya. Oleh karena itu, keamanan bukanlah sebuah pilihan, melainkan sebuah keharusan fundamental. Bagian ini menguraikan kerangka kerja Keamanan Operasional (OPSEC) yang komprehensif, yang mencakup analisis strategis terhadap taktik klandestin dan panduan praktis untuk keamanan fisik dan digital.

7.1 Kerangka Kerja OPSEC

Keamanan Operasional (OPSEC) adalah sebuah proses analitis yang digunakan untuk melindungi informasi dan aktivitas kritis dengan cara melihat diri sendiri melalui mata musuh (adversary). Ini bukan sekadar daftar alat, tetapi sebuah pola pikir yang disiplin dan konsisten. Untuk Studio Larang, proses OPSEC lima langkah dapat diadaptasi sebagai berikut:

1. Identifikasi Informasi Kritis (Critical Information-CI): Ini adalah informasi yang, jika diketahui oleh musuh, dapat membahayakan operasi atau para konspirator. Contoh CI untuk Egregore meliputi:
    - Identitas asli para konspirator.
    - Lokasi fisik di mana aktivitas klandestin (misalnya, pembajakan alat, penyimpanan material) terjadi.
    - Metode spesifik yang digunakan untuk "membajak" alat produksi tanpa terdeteksi.
    - Rincian keuangan, seperti total saldo kas atau alamat dompet kripto.

    - Rencana proyek di masa depan.
2. Analisis Ancaman (Threat Analysis): Mengidentifikasi siapa musuh dan apa kapabilitas mereka. Ancaman utama meliputi:
    - Pemilik Modal/Bos: Memiliki kepentingan untuk mencegah pencurian atau penggunaan tidak sah atas properti mereka. Kapabilitas mereka termasuk pengawasan di tempat kerja (CCTV, log akses) dan pelaporan ke pihak berwenang.
    - Aparat Negara (Polisi, Intelijen): Memiliki kapabilitas pengawasan yang luas, baik fisik maupun digital, dan wewenang penegakan hukum.
    - Informan/Penyusup: Individu yang mungkin menyusup ke dalam lingkaran afinitas untuk mengumpulkan informasi.
3. Analisis Kerentanan (Vulnerability Analysis): Mengidentifikasi kelemahan dalam praktik saat ini yang dapat dieksploitasi oleh ancaman. Contoh kerentanan:
    - Komunikasi yang tidak dienkripsi.
    - Kebiasaan yang dapat diprediksi (misalnya, selalu bertemu di tempat yang sama).
    - Jejak digital (misalnya, penggunaan media sosial, transaksi perbankan).
    - Kurangnya keamanan fisik di lokasi aktivitas.
4. Penilaian Risiko (Risk Assessment): Mengevaluasi kemungkinan setiap kerentanan dieksploitasi dan dampak yang akan ditimbulkannya. Risiko dihitung sebagai fungsi dari $Ancaman \times Kerentanan \times Dampak$. Ini membantu memprioritaskan tindakan penanggulangan.
5. Penerapan Penanggulangan (Countermeasures): Mengembangkan dan menerapkan tindakan spesifik untuk mengurangi risiko. Tindakan-tindakan ini dibahas secara rinci di bagian berikut.

7.2 Taktik Pembajakan dan Keamanan Fisik

Istilah "pembajakan" dan "sabotase" digunakan di sini dalam pengertian strategis sebagai tindakan perlawanan untuk merebut kembali alat produksi dari sistem kapitalis. Pelaksanaannya menuntut tingkat disiplin dan kehati-hatian yang tinggi.

7.2.1 Keamanan Fisik dan Kontra-Pengawasan

- **Manajemen Penampilan**: Saat melakukan aktivitas berisiko, konspirator harus secara aktif mengubah penampilan untuk mengalahkan sistem identifikasi. Ini termasuk mengenakan pakaian generik tanpa logo atau ciri khas, menutupi wajah dengan masker dan kacamata, menutupi rambut dan tato, dan bahkan mempertimbangkan untuk mengganggu pola jalan (misalnya, dengan kerikil di sepatu) untuk mengalahkan analisis gaya berjalan.
- **Kontra-Pengawasan Teknologi**: Kamera pengenal wajah semakin umum. Penggunaan LED inframerah (IR) atau near-infrared (NIR) yang dipasang pada kacamata atau tudung dapat secara efektif mengaburkan atau

membutakan kamera ini, terutama pada malam hari atau di area yang remang-remang.

- **Penghindaran Pola**: Musuh sering kali mengandalkan analisis pola untuk mendeteksi anomali. Konspirator harus menghindari rutinitas yang dapat diprediksi. Variasikan waktu, rute, dan lokasi untuk aktivitas yang sensitif.
- **Manajemen Aset Klandestin**: Bahan atau alat yang diperoleh melalui pembajakan harus disimpan di lokasi yang aman dan terpisah dari tempat tinggal atau aktivitas normal para konspirator. Harus ada pemisahan yang jelas antara persona "publik" dan persona "konspirator".

7.2.2 Pertahanan terhadap Rekayasa Sosial

Kelompok kecil yang erat sangat rentan terhadap penyusupan melalui rekayasa sosial (social engineering). Konspirator harus waspada terhadap taktik-taktik berikut:

- **Pretexting**: Penyerang menciptakan skenario atau dalih palsu untuk mendapatkan informasi atau kepercayaan. Contoh: seseorang yang mengaku sebagai simpatisan dan menanyakan detail operasional yang tidak perlu.
- **Phishing/Vishing/Smishing**: Upaya untuk menipu target agar mengungkapkan informasi sensitif (seperti kata sandi atau kunci privat) melalui email, panggilan suara, atau pesan teks palsu yang tampak sah.
- **Baiting**: Meninggalkan umpan fisik, seperti USB flash drive yang terinfeksi malware dengan label menarik ("Data Gaji"), di tempat yang kemungkinan besar akan ditemukan dan digunakan oleh target.

Pertahanan terbaik adalah pola pikir *zero-trust*: selalu verifikasi sebelum percaya. Jika seorang konspirator menerima permintaan yang tidak biasa atau mencurigakan, bahkan dari orang yang dikenal, verifikasi melalui saluran komunikasi kedua yang aman.

7.3 Keamanan Digital untuk Konspirator

Dalam era pengawasan digital massal, menjaga kebersihan digital (digital hygiene) adalah hal yang mutlak. Panduan berikut diambil dari praktik terbaik yang direkomendasikan oleh organisasi seperti Electronic Frontier Foundation (EFF) dan Frontline Defenders.

1. **Komunikasi Aman:**
    - Pesan Instan: Gunakan aplikasi dengan enkripsi ujung-ke-ujung (end-to-end encryption - E2EE) secara default, seperti Signal. Untuk anonimitas yang lebih tinggi, gunakan Session, yang merutekan pesan melalui jaringan terdesentralisasi dan tidak memerlukan nomor telepon untuk mendaftar.
    - Posel: Untuk komunikasi sensitif, gunakan penyedia posel (email) yang menawarkan E2EE, seperti TutaMail, RiseupMail, ProtonMail (tidak disarankan), atau konfigurasikan PGP (Pretty Good Privacy) secara manual. Hindari membahas informasi kritis melalui posel biasa. Kami menyarankan untuk menggunakan RiseupMail yang

dikerjakan oleh kolektif teknologi anarkis. Riseup tidak menyimpan log IP kita (termasuk dalam penggunaan VPN yang mereka buat), tidak seperti Proton yang bahkan pernah terjangkit semacam skandal. Meski begitu, ProtonMail tetap ditulis di sini karena akses dan pendaftarannya yang mudah. Setidaknya tetap lebih baik ketimbang posel biasa (seperti Gmail dan sebagainya).

2. **Keamanan Perangkat:**
    - Enkripsi Disk Penuh: Aktifkan enkripsi disk penuh di semua perangkat (BitLocker di Windows, FileVault di macOS). Untuk tingkat keamanan yang lebih tinggi, gunakan perangkat lunak open-source seperti VeraCrypt untuk membuat volume terenkripsi.
    - Kata Sandi & Otentikasi: Gunakan kata sandi yang panjang, unik, dan acak untuk setiap layanan. Kelola kata sandi ini menggunakan manajer kata sandi yang aman dan open-source seperti Bitwarden atau KeePass. Aktifkan Otentikasi Multi-Faktor (MFA) di semua akun yang mendukungnya, lebih baik menggunakan aplikasi authenticator (seperti Authy) atau kunci perangkat keras (seperti YubiKey) daripada SMS, yang rentan terhadap pembajakan SIM.
3. **Anonimitas Daring:**
    - Penjelajahan Web: Gunakan Tor Browser untuk semua aktivitas penjelajahan yang memerlukan anonimitas. Tor merutekan lalu lintas internet Anda melalui jaringan relawan global, membuatnya sangat sulit untuk melacak sumbernya.
    - VPN: Meskipun tidak memberikan anonimitas sekuat Tor, VPN (Virtual Private Network) yang terpercaya (dan berbayar) dapat menyembunyikan alamat IP Anda dari situs web yang Anda kunjungi. Hindari VPN gratis, karena model bisnis mereka sering kali melibatkan penjualan data pengguna.
    - Pemisahan Identitas: Buat identitas digital (email, akun media sosial) yang sepenuhnya terpisah untuk aktivitas konspirasi, dan jangan pernah mencampurnya dengan identitas pribadi Anda. Buat akun-akun ini saat menggunakan Tor atau VPN.
4. **Telepon Sekali Pakai (Burner Phones):**
    - Untuk komunikasi selama operasi berisiko tinggi, penggunaan burner phone sangat dianjurkan. Praktik terbaik meliputi:
        - Beli telepon murah dan kartu SIM prabayar secara tunai di tempat yang tidak memiliki pengawasan video yang ketat.
        - Jangan pernah menyalakan telepon ini di dekat rumah, tempat kerja, atau lokasi yang sering Anda kunjungi. Lakukan pengaturan awal di lokasi acak.
        - Jangan pernah memasukkan informasi pribadi atau masuk ke akun pribadi apa pun di telepon ini.
        - Hanya gunakan telepon ini untuk komunikasi terkait operasi, dan matikan saat tidak digunakan.

- Setelah operasi selesai, hancurkan telepon dan kartu SIM secara fisik. Jangan membawanya pulang.

Dengan menerapkan kerangka kerja OPSEC ini secara disiplin, para konspirator dapat secara signifikan mengurangi risiko deteksi dan represi, memungkinkan *Egregore Nomad-Cryptography* untuk beroperasi dan berkembang di dalam bayang-bayang.

8.0 Simpulan

Whitepaper ini telah menyajikan sebuah cetak biru yang komprehensif untuk *Egregore Nomad-Cryptography*, sebuah model eksperimental untuk otonomi sosio-ekonomi. Kerangka kerja ini secara unik mensintesis tiga domain yang berbeda menjadi satu kesatuan yang koheren: filsafat anarkis radikal, model ekonomi mutualis yang canggih, dan infrastruktur teknologi terdesentralisasi yang mutakhir. Ini bukan sekadar proposal teoretis; ini adalah panduan yang dapat ditindaklanjuti untuk para konspirator yang ingin memulai eksperimen mereka sendiri dalam kehidupan di luar kendali negara dan kapital.

Inti dari model ini adalah penolakan terhadap struktur formal dan hierarki. Dengan mengadopsi konsep Egregore sebagai entitas psikis yang emergent, TAZ sebagai modus operandi temporer, dan Pascakonspirasi sebagai etos afinitas yang terdesentralisasi, sistem ini dirancang untuk menjadi cair, adaptif, dan sulit dipahami oleh kekuasaan. Arsitektur ekonominya, yang berakar pada Mutualisme Proudhonian, menawarkan solusi konkret untuk masalah eksploitasi melalui kredit tanpa bunga dan kepemilikan sebagai kepenguasaan. Inovasi utamanya, Valuasi Kontribusi Multi-Atribut (VCMA), menyediakan metode yang adil dan bernuansa untuk mendistribusikan surplus berdasarkan kontribusi nyata—baik kualitatif maupun kuantitatif—sehingga menghargai semua bentuk kerja secara setara.

Infrastruktur teknis yang diusulkan—mulai dari perbendaharaan on-chain yang tahan sensor, penggunaan strategis aset kripto privat dan stabil, hingga integrasi kriptografi canggih seperti zk-SNARKs dan otomatisasi melalui Agen Ekonomi Otonom (AEA)—bukanlah sekadar hiasan teknologi. Setiap komponen dipilih secara khusus untuk memperkuat prinsip-prinsip filosofis yang mendasarinya: transparansi radikal, privasi absolut, dan otonomi yang tak tergoyahkan. Tata kelola melalui konsensus berbasis reputasi dinamis menawarkan jalan keluar dari tirani mayoritas, menciptakan sebuah meritokrasi cair di mana pengaruh diperoleh melalui partisipasi, bukan kekuasaan.

Namun, penting untuk menggarisbawahi kembali sifat eksperimental dari proyek ini. Seperti yang diperingatkan oleh Hakim Bey, TAZ harus menghilang begitu ia dipetakan dan dinamai untuk menghindari fosilisasi menjadi sebuah institusi. Keberhasilan *Egregore Nomad-Cryptography* tidak terletak pada kemampuannya untuk menjadi model permanen, melainkan pada kemampuannya untuk terus bergerak, berevolusi, dan jika perlu, dengan sengaja membubarkan diri untuk muncul kembali dalam bentuk yang baru dan lebih relevan. Ia harus

tetap menjadi sebuah "mesin perang" nomaden, bukan sebuah negara-kota yang menetap.

Pada akhirnya, otonomi sejati bukanlah sebuah tujuan akhir yang statis yang dapat dicapai sekali untuk selamanya. Ia adalah sebuah praktik perlawanan dan penciptaan yang terus-menerus, sebuah proses tanpa akhir. Kerangka kerja ini menyediakan seperangkat alat—filosofis, ekonomis, dan teknis—bagi mereka yang cukup berani untuk memulai perjalanan tersebut. Ini adalah undangan untuk berhenti menunggu revolusi dan mulai hidup di dalamnya, di sini dan sekarang, sebagai sebuah "pemberontakan permanen individu" yang menemukan kebebasannya dalam tindakan itu sendiri.

Daftar Pustaka

1) Aragorn. (2012). *Occupy everything: Anarchists in the Occupy Movement 2009-2011*.
2) Ashishpatel. (n.d.). *GitHub - ashishpatel26/500-AI-Agents-Projects: The 500 AI Agents Projects is a curated collection of AI agent use cases across various industries. It showcases practical applications and provides links to open-source projects for implementation, illustrating how AI agents are transforming sectors such as healthcare, finance, education, retail, and more.* GitHub. https://github.com/ashishpatel26/500-AI-Agents-Projects
3) Autonomys. (n.d.). *Releases · autonomys/autonomys-agents*. GitHub. https://github.com/autonomys/autonomys-agents/releases
4) Benello, C. G., Boyte, H. C., & Krimerman, L. (1992). *From the ground up: Essays on Grassroots and Workplace Democracy*.
5) Beresford, A. R., Patra, A., & Bellini, E. (2022). *Cryptology and network security: 21st International Conference, CANS 2022, Abu Dhabi, United Arab Emirates, November 13–16, 2022, Proceedings*. Springer Nature.
6) Bey, H. (2003). *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. Autonomedia.
7) Carson, K. A. (2007). *Studies in mutualist Political economy*. Booksurge Publishing.
8) De Filippi, P., Mannan, M., & Reijers, W. (2024). The rise of blockchain egregores. In *Research in the sociology of organizations* (pp. 129–136). https://doi.org/10.1108/s0733-558x20240000089011
9) Djoedibarie, I. (1979). *Post-conspiracy*. The Anarchist Library. Retrieved July 15, 2025, from https://theanarchistlibrary.org/library/itjang-djoedibarie-post-conspiracy
10) Dua, A., & Kumar, G. (2024). *Mastering zero-knowledge proofs: Practical study of security, scalability, and privacy in blockchain and modern systems (English Edition)*. BPB Publications.
11) Fetchai. (n.d.). *agents-aea/docs/aeas.md at main · fetchai/agents-aea*. GitHub. https://github.com/fetchai/agents-aea/blob/main/docs/aeas.md
12) Fleetwood, S. (1999). *Critical realism in economics: Development and Debate*. Psychology Press.

13) Frayne, C. T. (2022). Individualist Anarchism in France and Its Legacy [Apollo - University of Cambridge Repository]. https://doi.org/10.17863/CAM.80240
14) Groth, J., Kohlweiss, M., Maller, M., Meiklejohn, S., & Miers, I. (2018). Updatable and Universal Common Reference Strings with Applications to zk-SNARKs. In *Lecture notes in computer science* (pp. 698–728). https://doi.org/10.1007/978-3-319-96878-0_24
15) Keeney, R. L., Raiffa, H., & Rajala, D. W. (1994). Decisions with Multiple Objectives: Preferences and Value Tradeoffs. *Journal of the Operational Research Society*, *45*(9), 1093. https://doi.org/10.2307/2584151
16) Matiasmolinas. (n.d.). *GitHub - matiasmolinas/evolving-agents: Your toolkit for autonomous, evolving agent ecosystems. Create, execute, govern, and evolve agents that learn from experience, collaborate, build new capabilities, and operate safely within defined guardrails.* GitHub. https://github.com/matiasmolinas/evolving-agents
17) *Mutual aid.* (n.d.). The Anarchist Library. https://theanarchistlibrary.org/library/dean-spade-mutual-aid
18) Prichard, A. (2022). Pierre-Joseph Proudhon's Mutualist Social Science. In *Cambridge University Press eBooks* (pp. 286–307). https://doi.org/10.1017/9781108611022.013
19) Proudhon, P. (2007). *What Is Property?: An Inquiry into the Principle of Right and of Government.* https://theanarchistlibrary.org/library/pierre-joseph-proudhon-what-is-property-an-inquiry-into-the-principle-of-right-and-of-governmen.pdf
20) Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *IEEE Symposium on Security and Privacy.* https://doi.org/10.1109/sp.2014.36
21) Simular-Ai. (n.d.). *GitHub - simular-ai/Agent-S: Agent S: an open agentic framework that uses computers like a human.* GitHub. https://github.com/simular-ai/Agent-S
22) Steiner, A. (2019). *Les en-dehors: Anarchistes individualistes et illégalistes à la belle époque.*
23) Vincent, K. S. (2012). Property is theft! A Pierre-Joseph Proudhon anthology. *Anarchist Studies*, *20*(1), 121. https://www.questia.com/library/journal/1P3-2694731051/property-is-theft-a-pierre-joseph-proudhon-anthology
24) Wright, C. S. (2008). Bitcoin: a Peer-to-Peer electronic cash system. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3440802

Lampiran

Contoh Kode Smart Contract untuk Kas Afinitas (Solidity)

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.20;
```

```
import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/token/ERC20/IERC20.sol";

/**
 * @title AffinityTreasury
 * @dev A simple smart contract for managing the Egregore's affinity treasury.
 * It accepts funds from projects and allows for withdrawals based on governance proposals.
 * This is a simplified example and would require a more robust governance mechanism for production.
 */
contract AffinityTreasury is Ownable {
    IERC20 public acceptedToken; // e.g., DAI or a wrapped version of Monero
    mapping(bytes32 => bool) public executedProposals;

    event FundsDeposited(address indexed from, uint256 amount);
    event FundsWithdrawn(bytes32 indexed proposalId, address indexed to, uint256 amount);

    /**
     * @dev Sets the accepted ERC20 token for the treasury.
     * @param tokenAddress The address of the ERC20 token.
     */
    constructor(address tokenAddress) Ownable(msg.sender) {
        acceptedToken = IERC20(tokenAddress);
    }

    /**
     * @dev Function to deposit funds into the treasury.
     * Typically called by a project contract upon completion to transfer the 5% affinity cut.
     */
```

```
    function deposit(uint256 amount) external {

        require(acceptedToken.transferFrom(msg.sender, address(this), amount), "Token transfer
failed");

        emit FundsDeposited(msg.sender, amount);

    }



    /**

     * @dev Allows the governance mechanism (represented by the owner in this simplified version)

     * to withdraw funds based on a unique proposal ID.

     * A real implementation would use a multi-sig or a DAO governance contract.

     * @param proposalId A unique identifier for the governance proposal.

     * @param to The recipient of the funds.

     * @param amount The amount of tokens to withdraw.

     */

    function executeWithdrawal(bytes32 proposalId, address to, uint256 amount) external onlyOwner
{

        require(!executedProposals[proposalId], "Proposal already executed");

        require(to!= address(0), "Invalid recipient address");

        require(acceptedToken.balanceOf(address(this)) >= amount, "Insufficient funds");



        executedProposals[proposalId] = true;

        acceptedToken.transfer(to, amount);



        emit FundsWithdrawn(proposalId, to, amount);

    }



    /**

     * @dev Returns the current balance of the treasury.

     */

    function getBalance() external view returns (uint256) {
```

```
        return acceptedToken.balanceOf(address(this));

    }

}
```

Catatan: Kode di atas adalah contoh yang disederhanakan. Implementasi nyata akan menggantikan Ownable dengan kontrak tata kelola berbasis konsensus yang lebih kompleks.

Glosarium

1. Agen Ekonomi Otonom (AEA): Entitas perangkat lunak yang bertindak secara mandiri atas nama pemiliknya untuk mencapai tujuan ekonomi.
2. Egregore: Entitas atau kesadaran kolektif non-fisik yang muncul dari pikiran dan emosi bersama sekelompok individu.
3. FIPA-ACL: Foundation for Intelligent Physical Agents - Agent Communication Language. Sebuah standar protokol komunikasi antar-agen cerdas.
4. Kas Afinitas: Perbendaharaan bersama yang didanai oleh sebagian kecil surplus dari setiap proyek, digunakan untuk modal masa depan dan kebutuhan kolektif.
5. Konsensus Formal: Proses pengambilan keputusan di mana kelompok mencari kesepakatan yang dapat diterima semua pihak, tanpa pemungutan suara.
6. Kripto-Nomaden: Istilah yang menggabungkan penggunaan teknologi kriptografi ("Kripto") dengan filosofi mobilitas dan penghindaran strategis ("Nomaden").
7. MAUT (Multi-Attribute Utility Theory): Teori keputusan untuk mengevaluasi opsi berdasarkan beberapa kriteria atau atribut.
8. Mutualisme: Aliran pemikiran anarkis yang dipelopori oleh Proudhon, menekankan pada pertukaran yang adil, kredit mutual, dan kepemilikan sebagai kepenguasaan.
9. OPSEC (Operational Security): Proses analitis untuk melindungi informasi dan aktivitas kritis dari deteksi musuh.
10. Pascakonspirasi: Etos operasional yang menolak organisasi formal dan merangkul afinitas terdesentralisasi yang didorong oleh kepentingan individu.
11. TAZ (Temporary Autonomous Zone): Zona Otonom Temporer. Sebuah ruang dan waktu di mana kebebasan direalisasikan secara sementara, yang muncul dan menghilang untuk menghindari kontrol negara.
12. zk-SNARKs: Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge. Sebuah bentuk bukti kriptografi yang memungkinkan verifikasi suatu pernyataan tanpa mengungkapkan informasi rahasia yang mendasarinya